

юридичного факту, держава відносить його до кола комерційних суб'єктів, котрим житлово-будівельний кооператив не є ані до, ані після настання вказаної вище обставини.

Отже, державну податкову політику в частині оподаткування суб'єктів некомерційного господарювання – житлово-будівельних кооперативів навряд чи можна вважати такою, що спрямована на створення сприятливих умов для функціонування таких суб'єктів. Наразі податкове законодавство України містить у собі положення, що є дискримінаційними по відношенню до житлово-будівельних кооперативів та створюють перепони для розвитку кооперативного житлового будівництва, а відтак, і перепони на шляху відновлення України та розвитку її економіки.

Література:

1. Проект зі збору, оцінки й аналізу інформації про матеріальні втрати України від війни з Росією «Росія заплатить» URL: <https://kse.ua/ua/about-the-school/news/zagalna-suma-zbitkiv-zavdana-infrastrukturi-ukrayini-skladaye-ponad-127-mlrd-zvit-kse-institute-stanom-na-veresen-2022-roku/> (дата звернення: 08.11.2022).

2. Господарський кодекс України від 16.01.2003 р. № 436-IV. URL: <https://zakon.rada.gov.ua/laws/show/436-15#n753> (дата звернення: 08.11.2022).

3. Податковий кодекс України від 02.12.2010 р. № 2755-VI. URL : <https://zakon.rada.gov.ua/laws/show/2755-17#n12549> (дата звернення: 09.11.2022).

4. Лист № 1379/7/99-99-19-02-02-17 від 15.01.2016. Державна фіскальна служба України. URL: <https://tax.gov.ua/baneryi/podatkovii-konsultatsii/konsultatsii-dlya-yuridichnih-osib/print-66261.html> (дата звернення: 09.11.2022).

**Поліна Морозова, здобувач вищої освіти СВО Бакалавр;
Олена Єгорова, к.е.н., доцент,
доцент кафедри фінансів, банківської справи та страхування
Полтавський державний аграрний університет**

ВИДИ ФІНАНСОВОГО ШАХРАЙСТВА

Розвиток комп'ютерних, інформаційно-комунікаційних та інших технологій дає можливість люду розвиватись, надає безліч переваг їх користувачам, та поліпшує рівень життя. З іншої сторони він породжує велике розмаїття шахраїв та їхніх пасток, до яких щоденно потрапляють мільйони людей по всьому світу, шахрайство проникає до усіх сфер буття суспільства. Варто зазначити, що фінансові махінації набирають значних обертів і прогресують саме в онлайн середовищах. Оскільки повсякденне фінансове життя пересічного українця з кожним днем все більше переходить в Інтернет мережу, проводити такі афери злочинцям стає набагато простіше, швидше та вигідніше. Звісно, кожна людина повинна розуміти, що там, де обертаються

фінансові ресурси – завжди є небезпека і ризики повернути до себе надмірну увагу зі сторони шахраїв, тому бути обізнаним у фінансовій безпеці повинен кожен.

Фінансове шахрайство спостерігається у всіх майнових і грошових відносинах. Цей термін звикли асоціювати зі словом «крадіжка», але шахрайство полягає у присвоєнні чужого майна у більш прихованій формі.

Розглянемо найбільш розповсюджені види фінансового шахрайства:

1. Соціальна інженерія – це сукупність нетехнічних прийомів маніпулювання людьми, які використовуються кіберзлочинцями.

За допомогою цих прийомів шахраї отримують конфіденційні дані від жертв, які самі їх повідомляють. Вони включають махінації з персональними даними, у вигляді паролів та пін-кодів, які витягуються шляхом психологічного впливу на людину [2, с. 173]. Дані дії можуть відбуватися як телефоном, так і Інтернетом. Такий вид шахрайства вважається найрозповсюдженішим, він побудований на умовах довіри та удачі: повірить людина чи ні.

2. Скімінг – афера із банкоматами.

Цей різновид махінацій посідає другу сходинку у топі найпоширеніших методів фінансового шахрайства в Україні. Аферисти встановлюють до банкоматів та платіжних терміналів спеціальні пристрої (скімери), які викрадають дані банківських карток, що дозволяє у подальшому виготовити їх дублікати. Також доповненням слугують прикріплені мікрокамери, які фіксують PIN-код картки, який вводить власник [3]. Найбільше у пастку потрапляють ті картки, які мають магнітні стрічки, оскільки картки із чіпом та безконтактні захищені значно краще [2, с. 173].

До цієї групи шахрайських прийомів також можна віднести один із простіших, але не менш ефективніших методів, коли зловмисник чіпляє скотч на слот для видачі грошей. Не дочекавшись своїх коштів, які ніби застрягли в отворі, людина уходить без грошей, а аферисти збагачуються [2, с. 173].

Усі махінації з накладанням скімера на сьогодні вважаються вже застарілими. У наш час поширюються новітні апарати під назвою шимери, які є кращою та сучаснішою версією скімера. Боротися з скімерами набагато важче, оскільки звичайній людині складно їх побачити [4, с. 244].

3. Фішинг.

Також один із різновидів шахрайства у Інтернет середовищі, загальна схема якого наступна: на електронну адресу надходить сповіщення, у якому розміщено файл з вимогою надати облікову інформацію, перейшовши за посиланням [2, с. 173]. Усі відомості дуже добре скопійовані та викладені від імені ніби «банку», але фейкового. Якщо не бути уважним до дрібниць, то можна ввести свої конфіденційні дані, які одразу потраплять до рук шахраїв.

Споріднений до фішингу розглядають вішинг (голосовий фішинг), в якому відбувається та сама процедура з виманюванням особистих даних, але у телефонному режимі. Представляючись робітниками банку під різними приводами аферисти намагаються дізнатися важливу для них інформацію [4, с. 248].

4. Викрадення фінансового номеру телефону.

Вид фінансового шахрайства, у якому здійснюється перевипуск SIM-картки. Злочинці декілька разів дзвонять майбутній жертві, і навіть поповнюють телефонний рахунок, а потім звертаються до мобільного оператора і повідомляють про втрату сім-картки. Називаючи номери, з яких телефонували найчастіше, і суму, на яку заходили кошти, оператор ототожнює шахраїв з власником номера телефону. Після цього аферисти отримують повноцінний доступ до усіх даних, включаючи інтернет-банкінг та інформацію щодо платіжної картки [2, с. 173].

5. Фінансові піраміди.

У загальному розумінні фінансова піраміда – це фінансова будова, яка вербує коштами, її засновники обіцяють «інвесторам» високі прибутки, і виплачують дивіденди першим вкладникам за рахунок грошей, які прибувають від нових [1].

Переважно клієнтам обіцяють високі доходи за короткостроковий термін, але завжди змовчують про надмірні ризики [1]. Голови таких афер зазвичай вигадують неіснуючі послуги, а після того, як отримують кошти пропадають.

Для того, щоб захистити свої фінанси та не потрапити до пасток шахраїв, потрібно дотримуватись найпростішої фінансової безпеки, а саме: не розголошувати свої коди та паролі від банківської картки підозрілим особам (зокрема тим, хто називається представником банку); не відкривати листи, які надходять на електронну адресу від невідомих осіб та у жодному разі не намагатися перейти за посиланням; не реагувати на підозрілі повідомлення у соціальних мережах (навіть, якщо вони надіслані від друзів, зважайте, що їхні сторінки можуть бути зламани); не встановлювати неофіційні програми на пристрої, використовувати тільки програми з перевірених онлайн-платформ; завжди уважно оглядати банкомати перед тим як почати роботу з картою.

Отже, на сьогоднішній день шахрайство проводиться у великій кількості та є поширеним явищем. Спілкування людей призводить до виявлення усіх махінацій, які стають усе більш невідкладними для збагачення. Варто не забувати про методи застереження і бути пильним задля того, щоб поставити хрест на процвітанні подібної діяльності.

Література:

1. Арєф'єва І. Фінансова піраміда – що це і як її розпізнати? 2022. URL: <https://financer.com/ua/blog/finansovi-piramidy/>.

2. Гончар Л. В., Малахова А. В., Невкіпіла О. С. Фінансове шахрайство та безпека. *Науково-виробничий журнал*. Донецьк: 2021. С. 170–174.

3. Зятюк С. Як не втратити все: фінансова безпека у сучасному кіберпросторі. 2021. URL: https://zakordon.24tv.ua/yak-ne-vtratiti-vse-finansova-bezpeka-suchasnomu-ostanni-novini_n1652662.

4. Фінансова грамотність. Фінанси. Що? Чому? Як? : навч. посіб. / авт. кол. Київ : 2019. 272 с.